Neg May
IS490-Dr. Whitney
Final

As we gather here today, we face numerous challenges as the information gatekeepers for our organizations. Technology is changing the face of our businesses, from education to publishing to manufacturing, but we must always be prepared to meet these challenges head on. When we gathered here five years ago, we were faced with many of the same challenges that confront us today. However, in addition to these persistent concerns we also face a new set of obstacles erected in response to the rapidly changing geopolitical climate. These risks transcend those to physical security and have become intertwined with those traditionally confronting the information landscape. Not only are we managing the information storage, access, and retrieval, but we are also charged with a set of responsibilities of grave importance. While a brand new set of challenges faces us, and the state of information will change as soon as we leave this room, the prism through which we examine such risks will remain the same. While there are myriad mechanisms with which to analyze and assess where we are in the state of information, I can place them under the umbrella of what I like to call the "four pillars of the information environment."

Pillar One: Privacy

There is perhaps no issue that is as contentious as privacy. Unfortunately for us privacy governs much of the action we can take. There is considerable confusion as to what constitutes privacy and how we should approach it. In its most strict form, privacy is the

right to be secure in ones property and effects from government search or seizure. There is no firm basis upon which our ingrained right to privacy has been inured into the zeitgeist, but rather has evolved out of the country's founding principles. A litany of US Supreme Court cases in the latter half of the twentieth century added a considerable grey area to what constitutes a privacy right. To wit, Griswold v. Connecticut and Katz v. US circa 1960 built upon the cornerstone of Messrs. Samuel Warren and Louis Brande's 1890 Harvard Law Review treatise, "The Right to Privacy." Although they argued that invasion of privacy should be a civil tort, their work laid the cornerstone of what has become an immense body of confusing and often contradictory law. Privacy concerns in our organizations are ubiquitous, but they are even more challenging in our profession particularly for those of us in academia. Student information has always been held close to the vest – not to mention the payroll, human resource, and recruiting data.

We have addressed these concerns in the past by investing in hardware and by restricting access to and training those responsible for sensitive information. But the current state of information has made tools available to us that allow us to harness information whie ostensibly storing information for otherwise legitimate reasons. Every one of us in this room would like to know more about our customers. The University's 'onecard' could be considered a significant privacy concern if it were used in such a manner. The card could be used to track the buildings to which a student gains access, what he eats for breakfast, what CD he purchases, and even what time of day he visits the gym. Many of you could do the same with employee access cards or customer loyalty cards designed to integrate with other databases available in the marketplace.

On one hand we must balance the privacy interests of the student with the responsibilities of the University. As we become a more entrepreneurial enterprise, the University is not unlike those of you out there who operate a more traditional market oriented business. Many consumers wish to minimize such information in the hands of an organization, but what are our obligations to voluntarily abrogate our fiduciary responsibility to develop our customers as lifelong clients? The technology is available but we have thus far refrained from using it while we struggle with these sensitive issues. I am, however, a strong advocate of allowing the consumer to choose what information he divulges. Due to the nature of our customer base and the costs associated with analyzing the information, I would not be inclined to maintain a centralized repository of superfluous student information.

In addition to these difficult internal information struggles, exogenous circumstances create other challenges. As a result of the country's principled commitment to protecting its citizens against terrorist organizations, we have been charged with providing information about international students. Although it is an extra burden on our staff that has significant workload already, it is a charge that I will keep.

Pillar Two: Intellectual Property

Intellectual property concerns are a challenge for any organization, but are particularly troublesome for universities. We must deal with intellectual property concerns in our libraries, with our researchers, and from our students and staff.   Although the idea of

copyright can be found in the US Constitution, the protection did not extend in practice until the late 1800's (Whitney Lesson 7). With such a vast array of subjects under its purview it is important to understand what is and isn't intellectual property. The World Intellectual Property Organization (WIPO 1998) defines intellectual property as the means the legal rights which result from intellectual activity in the industrial, scientific, literary and artistic fields. The operative phrase in that definition, of course, is intellectual activity. This is a very broad statement in that we are in the business of fostering intellectual activity. Is it prudent to extend a copyright to every classroom session or to Board of Trustee meetings? Of course not, and thankfully in 1976 the US Congress stepped in to help us figure that out.

The fair use doctrine affects every one of us in the room. It allows for reproduction of copyrighted material for purposes such as criticism, reporting, and instructing. Some courts have circumvented the legislative process and have created additional 'subsections' to the law by judicial fiat. They aren't really subsections but opinions that have created new rules under the fair use doctrine that have become so voluminous that compliance has become a significant challenge. For example, some courts have ruled that an 'element of spontaneity' is necessary. This would suggest that a teacher may use a case from the morning paper to stimulate discussion, but would have to obtain approval from the paper to discuss a case from the prior year's edition. These issues have become so complex that our university has created an office of copyright compliance within the general counsel's office, which must approve all teaching materials before they are used.

On the other side of the fair use coin is our interest in protecting the copyright interests of our researchers employed at the University. Our faculty members expend a considerable amount of effort publishing journal articles, magazine articles, and the like. Our academic reputation is contingent on the quality and scope of the research we direct. We also employ faculty and staff members in the literary, art, and music fields whose work must be protected. This implies a delicate balance between what constitutes fair use when our own employee's work is in question. This in part is a primary reason why we have taken such an aggressive stand on complying with the fair use doctrine in our teaching materials.

While complying with fair use is one of our greatest challenges today, the legacy of the Digital Millennium Copyright Act (DMCA) is one of the most significant variables that we face. It is difficult to accurately assess the state of information when this eight hundred pound gorilla has not fully materialized- it usually takes decades for the law of unintended consequences vis-à-vis significant government regulation to play out. The DMCA is one of the most comprehensive copyright reforms in a generation, and the implications of the law will be great. As literary works and software are increasingly distributed in digital format, the DMCA will most likely ensure that more works come with license agreements and the stipulation to pay for each access. We have become accustomed to following the licensing model in the software arena, but this presents a significant obstacle to the traditional library paradigm when extended beyond software, which can be designated to a particular machine for a particular user. All of us who are responsible for archiving and providing access to information must be prepared to

scrutinize contracts for the acquisition of digital works more than ever before and be prepared to negotiate terms for fair access in all foreseeable circumstances.

This brings us to the final point I would like to make regarding intellectual property and that is distance education. We are intensely focused on the relationship between intellectual property and distance learning, and in my estimation all organizations should. All of our organizations have come a long way in educating our workforce, and I would venture to bet that most if not all of you have some sort of distance based training programs for your employees. The DMCA did not expand protection for educational activities over the Internet, and this medium will continue to be stifled until Congress addresses the issue in a favorable manner. Without such exemption it would be virtually impossible to expand the breadth of distance education systems, as obtaining permission for copyrighted works is untenable and the cost for licensing such works is prohibitive. We do not foresee the day when the norm for educational instruction extends beyond the classroom walls. It will continue to be a minor component of the educational portfolio, but it could be vastly enhanced with such permissions.

Pillar Three: Information Ethics

Before concluding with what I deem to be the most important component of the information environment, I must broach the subject of information ethics. Ethics is inextricably intertwined with intellectual freedom, my concluding pillar, in that any limit to intellectual freedom is itself an ethical paradox. For proof one need only examine the

main ethical question posed by The International Center for Information Ethics. "The main ethical question in this field may be formulated as follows: Are there limits to intellectual freedom?" (http://icie.zkm.de/research). Since 1930 (ALA 1930), the library profession has acknowledged the unique role they play in society. As a University we play a very similar role, and those of you out there in the private sector must also adopt a code of ethics. For, a code of ethics is much more than a historical document, but it is also a process (Whitney Lesson 11).

We must consider more than the ethos of the library profession. Our organizations are diverse workplaces represented by employees of many different professions. We employ lawyers, accountants, marketers, and other professionals who are guided by their own professional codes of ethics. Sometimes an employee's professional ethics will contradict your organization's ethics. This manifests in our organization, as it does in many, with respect to the information that is made available to employees. Censorship, for the most part, is anathema to the information professional. However, we strive to maintain an appropriate workplace in that the potential legal liability and embarrassment to the organization far outweighs the ideals of the information professional. The code of ethics is a guiding principle – it is not a suicide pact. As the stewards of information, we as professionals must advocate adherence to the code of the information professional, but we must not forget our duty to the wellbeing of the organization. Our role as information stewards imparts a significant and vast responsibility upon us. We are members of a profession that is committed to intellectual freedom and free access to information. We

must remember our professional commitments while we shape the overall organizational policies.

Pillar Four: Intellectual Freedom

We certainly live in interesting times. The past 15 months has seen a drastic change of our society, and the country's consideration of the balance between security and intellectual freedom has not yet been firmly woven into the fabric of our country's acceptable mores. After all, it took about six years from the Articles of Peace to the Bill of Rights for our country's greatest thinkers to formally recognize the right to free expression. To take this basic ideal of intellectual freedom from the writings of John Locke (Milton 1996) and his ilk to enumeration in our country's founding documents was the lynchpin of spreading freedom around the world.

The past 15 months has, unfortunately, seen a lot of disinformation concerning the state of information. We all have our conceptions concerning the value of intellectual freedom- we would not be in this room if we were not only dedicated to the freedom of our ideas, but also recognized the value of protecting that freedom. It is easy to define intellectual freedom as an absolute free market of ideas free of impediment. Thus, I would like to dedicate some time to setting the record straight regarding the prevailing political tide as it relates to intellectual freedom.

As long as ideas have been around so has censorship in some form, thus intellectual freedom in its purest form has never really existed. But there has never been capitalism in its purest from for that matter and that does not preclude us from aspiring to achieve that goal. Intellectual freedom is a fundamental right that is all but guaranteed in the spirit of the First Amendment. For more than 200 years intellectual freedom has been considered a basic human right in this country, and that is one of the principal reasons our country remains the greatest bastion of wealth and freedom in the history of the world. But we confront different challenges than we did when this country was founded. Gone are the days when the primary conduit to intellectual freedom was the printing press and the repositories of information were journals and catalogs born out of the labor of the human hand.

Some would compare the information gathering initiatives of the United States government to Orwell's Oceania. Putting aside the hackneyed comparison that can be made to just about any contemporary government (Hitchens 2002), this simplistic charge shirks one's responsibility to rigorously analyze the role of an organization in the face of changing domestic, geopolitical, and technological climates. Gone are the days when the government could not retain newspaper clippings about dangerous organizations. There is a delicate balance between protecting the freedom to espouse one's beliefs and legitimately gathering information to thwart criminal activity. And much of the responsibility is falling on us.

One of the responsibilities with which academic organizations has been charged is the responsibility to track foreign students to ensure that they are actually attending classes at the institution that they indicate on their visa application. This simple act of verification may be mischaracterized by civil liberties groups but it is a rather innocuous administrative task. The challenge for us is to update our systems to meet this requirement while ensuring that those responsible for performing this task do not abuse the information to which they require access. Most of our organizations rely heavily on foreign students and employees. Therefore, we must not alienate them and be cognizant of their sensitivities. But we must also realize that the changing dynamics of the information environment are such that our compliance may thwart those with evil intentions. We are not acting as agents of the government – far from it. Confirming registration at our organizations is not stifling intellectual freedom in any manner- the fruits of our labor bear a safer society.

The flurry of regulation since September 11, 2001 has placed our organizations in circumstances never before encountered by the information profession. Part and parcel of a university's mission is to promote the intellectual freedom and development of its students. One particular piece of legislation passed in the rush to secure our homeland is the Cyber Security Enhancement Act of 2002(HR 107-3682). At first glance it seems to do nothing more than protect government agencies against hackers. But, section 102 requires that organizations turn over the contents of email or other electronic correspondence to *any* government entity that have a good faith belief that an emergency constituting serious physical injury or death is at hand.

Again those who have been quick to fear monger have latched on to this piece of legislation as "proof" of Oceania's- I mean the US government's- evil intentions. (These are incidentally some of the same people who don't mind if the country's chief law enforcement officer commits perjury in a civil deposition or side with one of the world's most maniacal and homicidal dictators- but that's a different speech). Although I would be derelict in my duty to suggest that our organizations should hand over the details of our community's electronic correspondence, I would be even more negligent if I were to paint intellectual freedom with such a broad brush. I submit to you:

Is scheming to assassinate a government official intellectual freedom?

Is funneling money to a terrorist organization intellectual freedom?

Is conspiring to blow up an academic building intellectual freedom?

I would venture to guess that most of you answered 'no' to these questions. You answered 'no' for good reason; because you are right. In order to foster and develop a sense of intellectual freedom we must understand what it is. I would like you to consider the ALA's definition: "… intellectual freedom encompasses the freedom to hold, receive and disseminate ideas." It's easy for us to get so consumed with the 'freedom' part of the equation that what is often lost, and I hope that I have conveyed this evening, is that intellectual freedom is about *ideas*. We must not allow ourselves to aid those who wish us ill because there are those who are not equipped with the intellect to discern ideas from criminal acts.

Concluding Remarks

Determining the state of the information environment is a challenging task in that it is a rapidly moving target. We are forced to deal with a challenging environment that would have been unthinkable only a decade earlier. Often we must balance competing interests as we set out to accomplish our goals. But I hope that I have imbued you with the overarching concerns that must be at the forefront of the mindset of every information professional. Intellectual freedom and privacy considerations are paramount to the success of our organizations, but we must not be so wrapped up in protecting all ideas, regardless of their treachery, that we lose sight of what we are supposed to be promoting. And that's the reason that information ethics is the cohesive unit that binds our profession and defines where we are in the state of information. We are, on the whole, following an ethical course, although new situations require unique responses. Reasoned arguments can be advanced for excessive intrusion into privacy or for curbing intellectual property. On the other side of the coin, there are reasoned arguments suggesting a completely free market of ideas, unimpeded by the government. Our moral compass embodied in our sense of ethics is helping us balance the competing interests and helping us form a society that promotes a well regulated, but very open free market of ideas. And that is the state of information.

Endnotes

Abbott, S. (2002). Out of Utah does Brigham Young University pose a threat to academic

freedom? The Boston Globe. October 27 p. D1.

American Library Association (1930). Suggested Code of Ethics. American Library

Association Bulletin (24) 58-62.

Association of College & Research Libraries (1999). Intellectual Freedom Principles for

Academic Libraries.

Egelko, B. (2002). FBI snooping has librarians stamping mad. The San Francisco

Chronicle. September 16 p. A15.

Hitchens, C. (2002). Why Orwell Matters. Basic Books.

Kurtz, S. (2002). Through the FIRE. The National Review. September 19. p.15-20.

Markoff, J. (2002) Pentagon plans a computer system that would peek at personal data of

Americans. New York Times. November 9, p. A1.

Milton, J. R. (1996). Lockean political apocrypha. British Journal for the History of

Philosophy (4) 247-266.

Parkes, C. (2002). Intellectual freedom fighters take on Disney. The Financial Times.

October 12 p. 7.

Slaton, J. (2002). Homeland insecurity: Is your privacy in danger? The San Francisco

Chronicle. December 12, p. A1.

World Intellectual Property Organization. (2001). WIPO intellectual property handbook.

WIPO publication no. 489. Geneva.

US Copyright Office. (1998). The Digital Millennium Copyright Act of 1998: US

Copyright Office Summary.